



**Prioritätsbescheinigung über die Einreichung
einer Patentanmeldung**

Aktenzeichen: 101 40 721.1

Anmeldetag: 27. August 2001

Anmelder/Inhaber: Bayerische Motoren Werke Aktiengesellschaft,
80809 München/DE

Bezeichnung: Verfahren zur Bereitstellung von Software zur Ver-
wendung durch ein Steuergerät eines Fahrzeugs

IPC: B 60 R 16/02

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ur-
sprünglichen Unterlagen dieser Patentanmeldung.

München, den 12. Februar 2004
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

**CERTIFIED COPY OF
PRIORITY DOCUMENT**

Verfahren zur Bereitstellung von Software zur Verwendung durch ein Steuergerät eines Fahrzeugs

Beschreibung

Die Erfindung betrifft insbesondere ein Verfahren zur Bereitstellung von Software zur Verwendung durch ein Steuergerät eines Fahrzeugs, wie insbesondere ein Kraftfahrzeug oder Motorrad, nach dem Oberbegriff des Anspruchs 1.

Steuergeräte für Kraftfahrzeuge weisen üblicherweise eine durch Software gesteuerte Ablaufsteuerung auf, die nach der Herstellung des Steuergeräts beim Hersteller des Steuergeräts oder beim Fahrzeughersteller nach der Montage des Steuergeräts in diesem gespeichert wird.

Nachteilig ist, dass die Software in schädigender Weise, ausgetauscht oder abgeändert werden kann.

Die Aufgabe der Erfindung besteht in der Verbesserung der Software/Hardware-Kombination, wie insbesondere eines Kraftfahrzeugs oder Personenkraftwagens.

Diese Aufgabe wird durch die in den unabhängigen Patentansprüchen angegebenen Maßnahmen jeweils gelöst. Vorteilhafte Ausgestaltungen der Erfindung sind in den abhängigen Patentansprüchen angegeben.

Ein wichtiger Aspekt der Erfindung besteht darin, unter Verwendung des Public-Key-Verfahrens, eine zur Verwendung durch ein Steuergerät eines Fahrzeugs vorgesehene Software, wie insbesondere ein Kraftfahrzeug oder Motorrad, unter Verwendung des geheimen bzw. privaten Schlüssels einer Software-Signaturstelle gegen Verfälschung zu signieren. Das Public-Key-Verfahren zeichnet sich insbesondere dadurch aus, dass es von einem besonderen Schlüssel-Paar Gebrauch macht, nämlich einem geheimen, privaten Schlüssel und einem zu diesem komplementären öffentlichen Schlüssel.

Alternativ oder ergänzend ist bei einer weiteren Ausführungsform der Erfindung vorgesehen, ein Software-Signatur-Zertifikat unter Verwendung des öffentlichen Schlüssels der Software-Signaturstelle und des geheimen Schlüssels einer Kontrollinstanz, eines sogenannten Trust-Centers, im Rahmen eines Public-Key-Verfahrens, zu erzeugen.

Alternativ oder ergänzend ist bei einer weiteren Ausführungsform der Erfindung vorgesehen, ein Kontrollinstanz-Zertifikat bzw. Trust-Center-Zertifikat unter Verwendung des geheimen Schlüssels der Kontrollinstanz zu erzeugen.

Alternativ oder ergänzend ist bei einer weiteren Ausführungsform der Erfindung vorgesehen, Freischaltcode-Daten unter Verwendung des geheimen Schlüssels einer Freischaltcode-Stelle im Rahmen eines Public-Key-Verfahrens zu signieren.

Alternativ oder ergänzend ist bei einer weiteren Ausführungsform der Erfindung vorgesehen, ein Freischaltcodestelle-Signatur-Zertifikat unter Verwendung des geheimen Schlüssels der Kontrollinstanz, des Trust-Centers, im Rahmen eines Public-Key-Verfahrens, zu erzeugen.

Alternativ oder ergänzend ist bei einer weiteren Ausführungsform der Erfindung vorgesehen, das Trust-Center-Zertifikat in einer gegen Verfälschung und/oder Austausch geschützten Weise, wie in einem geschützten Speicher, Speicherbereich oder dgl., in dem Steuergerät zu speichern.

Alternativ oder ergänzend ist bei einer weiteren Ausführungsform der Erfindung vorgesehen, das Freischaltcodestelle-Signatur-Zertifikat, das Software-Signatur-Zertifikat, die Freischaltcode-Daten und deren Signatur sowie die Software und deren Signatur in dem Steuergerät zu speichern.

Alternativ oder ergänzend ist bei einer weiteren Ausführungsform der Erfindung vorgesehen, dass das Software-Signatur-Zertifikat eine oder mehrere Gültigkeitsbeschränkungen, wie insbesondere eine Beschränkung auf einen oder mehrere Steuergerätetypen, aufweist.

Alternativ oder ergänzend ist bei einer weiteren Ausführungsform der Erfindung vorgesehen, dass das Freischaltcodestelle-Signatur-Zertifikat eine oder mehrere Gültigkeitsbeschränkungen aufweist, wie insbesondere eine Beschränkung auf ein bestimmtes Steuergerät, das beispielsweise anhand einer in diesem unveränderlich gespeicherten Nummer, Kennung oder dgl. individualisiert ist, oder die Fahrgestellnummer eines Fahrzeugs.

Alternativ oder ergänzend ist bei einer weiteren Ausführungsform der Erfindung vorgesehen, dass das Software-Signatur-Zertifikat im Rahmen eines Public-Key-Verfahrens unter Verwendung des öffentlichen Schlüssels des Trust-Centers auf Unverfälschtheit überprüft wird.

Alternativ oder ergänzend ist bei einer weiteren Ausführungsform der Erfindung vorgesehen, dass die signierte Software im Rahmen eines Public-Key-Verfahrens unter Verwendung des im Software-Signatur-Zertifikat enthaltenen öffentlichen Schlüssels der Softwaresignatur-Stelle auf Unverfälschtheit überprüft wird.

Alternativ oder ergänzend ist bei einer weiteren Ausführungsform der Erfindung vorgesehen, dass das Freischaltcodestelle-Signatur-Zertifikat im Rahmen eines Public-Key-Verfahrens unter Verwendung des öffentlichen Schlüssels des Trust-Centers auf Unverfälschtheit überprüft wird.

Alternativ oder ergänzend ist bei einer weiteren Ausführungsform der Erfindung vorgesehen, dass die signierten Freischaltcode-Daten im Rahmen eines Public-Key-Verfahrens unter Verwendung des im Freischaltcodestelle-Signatur-Zertifikats enthaltenen öffentlichen Schlüssels der Freischaltcodestelle auf Unverfälschtheit überprüft werden.

Alternativ oder ergänzend ist bei einer weiteren Ausführungsform der Erfindung vorgesehen, dass das Steuergerät mit einem ablaufgesteuerten Mikroprozessor versehen ist, der eines der vorstehend beschriebenen Verfahren unter Verwendung des Public-Key-Verfahrens ausführt.

Die Erfindung wird nachfolgend anhand einer Zeichnung näher erläutert, wobei gleiche Bezugszeichen gleiche oder gleichwirkende Maßnahmen angeben. Es zeigt:

Fig. 1 eine graphische Veranschaulichung eines erfindungsgemäßen Verfahrens zur Bereitstellung von Software zum Betrieb eines Steuergeräts in einem Fahrzeug, wie insbesondere ein Kraftfahrzeug oder Motorrad.

Bei dem in Figur 1 dargestellten Ablaufschema 100, das von dem bekannten Public-Key-Verfahren Gebrauch macht, wird ein Programm-Code zur Ablaufsteuerung eines Steuergeräts 115, d.h. eine Steuergerät-Software 113, an eine sogenannte Software-Signaturstelle 105 zum Zwecke seiner Signatur übermittelt. Bei dem Steuergerät 115 handelt es sich um eine programmgesteuerte Datenverarbeitungseinrichtung, die bevorzugt einen programmierbaren Speicher und einen Mikroprozessor aufweist. Anhand der Signatur kann erkannt werden, ob der Programm-Code nach der Signatur verändert bzw. manipuliert worden ist. Wie dies geschieht, wird im Folgenden näher erläutert.

Unter einem Steuergerät soll insbesondere sowohl ein herkömmliches Steuergerät in einem Fahrzeug zum Steuern und/oder Regeln von Aktuatoren als auch die sonstige programmgesteuerte Ausstattung eines Fahrzeugs verstanden werden, wie beispielsweise ein Kommunikations-System, ein Audio-System oder ein Navigations-System. Obwohl derzeit eine Vielzahl von Steuergeräten für unterschiedliche Funktionen bzw. Aktuatoren in Fahrzeugen vorgesehen sind, kann es sich bei einem erfindungsgemäßen Steuergerät auch um ein oder mehrere programmgesteuerte Datenverarbeitungseinrichtungen handeln, die die Steuer- und/oder Regelaufgaben von mehr als einem Steuergerät übernehmen.

Die Software-Signaturstelle 105 fordert bei einem sogenannten Trust-Center 101 des Fahrzeugherstellers, für dessen Fahrzeug das Steuergerät 115 bestimmt bzw. in dessen Fahrzeug es eingebaut ist oder werden soll, ein Software-Signatur-Zertifikat 120 an. Bei der Software-Signaturstelle 105 handelt es sich bevorzugt um den Hersteller der Software 113, wobei dies bevorzugt auch der Hersteller des Steuergeräts 115 ist.

Unter Verwendung seines nicht-öffentlichen, privaten Schlüssels 103 sowie des öffentlichen Schlüssels 108 der Software-Signaturstelle 103 erzeugt das Trust-Center 101 das Software-Signatur-Zertifikat 120. Dieses weist insbesondere den öffentlichen Schlüssel 108 der Software-Signaturstelle 105, bevorzugt ein oder mehrere Gültigkeitsbeschränkungen, die nicht explizit dargestellt sind, und eine von dem Trust-Center 101 erzeugte Signatur 121 auf. Die Signatur ermöglicht die Überprüfung, ob das Zertifikat nach seiner „Unterzeichnung“ bzw. Signatur verändert oder manipuliert worden ist.

Bei einer von dem Steuergerät 115 auf ihre Erfüllung hin überprüften Gültigkeitsbeschränkung im Software-Signatur-Zertifikat 120, kann es sich insbesondere um eine Beschränkung betreffend eine Betriebsstundenzahl, eine Lauf- bzw. Kilometer-Leistung, eine örtlich begrenzte Gültigkeit (in Bezug auf den Aufenthaltsort des Fahrzeugs), eine Zeitangabe oder Zeitdauer, ein oder mehrere Fahrzeugtypen, ein oder mehrere Steuergeräte oder Steuergerädetypen, eine Fahrgestellnummer oder eine Steuergerätenummer handeln. Bevorzugt weist das Software-Signatur-Zertifikat eine Beschränkung der Verwendbarkeit der Software auf ein oder mehrere Steuergerädetypen auf. Eine weitere Beschränkung kann darin bestehen, dass der Hersteller einer Software diese nur dann in ein Steuergerät einschreiben bzw. dort speichern oder zum Ablauf bringen kann, wenn der Hersteller der Software auch der Hersteller des Steuergeräts ist. Die Überprüfung der ein oder mehreren Gültigkeitsbeschränkungen erfolgt bevorzugt durch einen im Steuergerät 115 vorgesehenen, ablaufgesteuerten Mikroprozessor (nicht dargestellt), wobei dessen Ablaufsteuerung bzw. Software, entsprechend gestaltet ist.

Das Trust-Center 101 erzeugt ferner unter Verwendung seines geheimen Schlüssels 103 ein Trust-Center-Signatur-Zertifikat 116, das insbesondere dessen öffentlichen Schlüssel 101 und eine unter Verwendung des geheimen Schlüssels 103 des Trust-Centers 101 erzeugte Signatur 117 aufweist.

Die Software-Signaturstelle 105 erzeugt unter Verwendung ihres privaten bzw. geheimen Schlüssels 109 und der Software 113 eine Signatur 114, anhand der vom Steuergerät, wie insbesondere durch einen programmgesteuerten Mikroprozessor,

überprüft werden kann, ob die Software 113 nach deren Signierung mit der Signatur 114 verändert worden ist.

Die Zertifikate 116 und 120 sowie die Software 113 und deren Signatur 114 werden in das Steuergerät 115 übertragen und dort gespeichert. Die Speicherung des Trust-Center-Signatur-Zertifikats 116 erfolgt in einem geschützten Speicher oder Speicherbereich 122, der verhindert, dass das Trust-Center-Signatur-Zertifikat 116 verändert und/oder ausgetauscht werden kann.

Wenn der Hersteller der Software und der Hersteller des Steuergeräts identisch sind, geschieht dies ganz oder teilweise bevorzugt durch den Hersteller vor der Auslieferung des Steuergeräts an den Fahrzeughersteller.

Zur Aktualisierung der im Steuergerät gespeicherten Software oder zur Bereitstellung von zusätzlicher oder alternativer Software im Steuergerät 115 können erfindungsgemäß mehrere Wege zum Einbringen der Software in das Fahrzeug verwendet werden. Dies kann beispielsweise bei einem Werkstattbesuch, z.B. über einen Diagnosestecker oder ein Kommunikations-Interface des Fahrzeugs, oder auch von einem an den Fahrzeugbesitzer ausgehändigten Datenträger, wie eine CD-ROM, DVD oder Chipkarte, erfolgen. Die Software wird dann ggf. über ein im Kraftfahrzeug vorgesehenes Lesegerät für den betreffenden Datenträger eingespielt.

Bevor das Steuergerät 115 die an das Steuergerät 115 übertragene Software 113, ausführt, prüft das Steuergerät 115 in einem ersten Schritt auf der Basis des Public-Key-Verfahrens unter Verwendung des Software-Signatur-Zertifikats 120, das den öffentlichen Schlüssel 108 der Software-Signatur-Stelle 105 und die Signatur 121 des Trust-Centers 101 aufweist, und unter Verwendung des im geschützten Speicher oder Speicherbereich 122 gespeicherten öffentlichen Schlüssels 102 des Trust-Centers 101, ob das Software-Signatur-Zertifikat 120 verändert bzw. manipuliert worden ist.

Falls dies nicht der Fall ist, prüft das Steuergerät in einem zweiten Schritt auf der Basis des Public-Key-Verfahrens unter Verwendung des öffentlichen Schlüssels 108 der Software-Signatur-Stelle 105, der im ersten Schritt unter Verwendung des

öffentlichen Schlüssels 102 des Trust-Centers 101 auf seine Unverändertheit hin überprüft worden ist, sowie unter Verwendung der Software 113 und der Signatur 114, ob die Software 113 verändert bzw. manipuliert worden ist.

Die positiv verlaufende Prüfung im ersten und zweiten Schritt, vorzugsweise von einem Prozessor (nicht dargestellt) des Steuergeräts, ist bei dem hier nachfolgend beschriebenen Ausführungsbeispiel eine erste notwendige jedoch nicht hinreichende Voraussetzung, damit die Software 113 von dem Steuergerät 115 ausgeführt werden kann.

Bevorzugt wird beispielsweise von dem Steuergerät 115 bzw. einem in diesem vorgesehenen ablaufgesteuerten Mikroprozessor (nicht dargestellt) zudem überprüft, ob eine oder mehrere bevorzugt im Software-Signatur-Zertifikat 120 von dem Trust-Center 101 hinterlegte Gültigkeitsbeschränkungen bzw. Gültigkeitsvoraussetzungen, wie insbesondere eine Betriebsstunden-Beschränkung der Verwendbarkeit des Zertifikats 120, erfüllt sind. Ggf. bildet die Erfüllung der Gültigkeitsbeschränkungen bzw. Gültigkeitsvoraussetzungen eine weitere Voraussetzung, damit die Software 113 von dem Steuergerät 115 ausgeführt werden kann.

Bei einem anderen Ausführungsbeispiel, auf das nicht weiter eingegangen wird, handelt es sich hierbei um die alleinigen bzw. hinreichenden Voraussetzungen für die Ausführung der Software durch das Steuergerät.

Falls nicht bereits im Steuergerät 115 oder im Fahrzeug gespeichert, wird die signierte Software, die die Steuergerät-Software 113 und die Software-Signatur 114 aufweist, und das mit dem öffentlichen Schlüssel 108 versehene Software-Signatur-Zertifikat 120, ggf. mit weiterer Software, dem Besitzer eines Fahrzeugs auf einem Datenträger (nicht dargestellt), wie eine CD-ROM oder DVD, zur Verfügung gestellt. Auf dessen Dateninhalt kann beispielsweise über eine entsprechende Datenverarbeitungseinrichtung (nicht dargestellt), die mit mindestens einem Steuergerät eines Kraftfahrzeugs in Verbindung steht, zugegriffen werden.

Im Folgenden wird angenommen, dass der Benutzer von der durch eine auf dem Datenträger verfügbaren Software bzw. von der dadurch gebotenen Zusatz-

Funktionalität Gebrauch machen und die Software dementsprechend in ein oder mehrere Steuergeräte laden und dort ablaufen lassen möchte.

Bei dem hier behandelten, bevorzugten Ausführungsbeispiel sind zu den vorgenannten Schritten zusätzliche Schritte erforderlich bzw. Voraussetzungen zu erfüllen. Im hier geschilderten Ausführungsbeispiel nimmt der Besitzer des Fahrzeugs telefonisch oder per Internet aus dem Fahrzeug heraus Kontakt mit einer sogenannten Freischalt-Code-Stelle 104 auf. Nachdem die Zahlungsmodalitäten geklärt worden sind, wählt der Besitzer die betreffende freizuschaltende Software aus, übermittelt die Fahrgestellnummer und/oder eine das betreffende Steuergerät kennzeichnende Nummer oder dgl. (wobei dies auch elektronisch durch Auslesen und Übermittlung aus den betreffenden ein oder mehreren Steuergeräten geschehen kann) und gibt im Falle einer zeitabhängigen Nutzungsgebühr für die Software an, für welchen Zeitraum er die Nutzung der Software wünscht. Auf der Basis dieser Nutzungs-Angaben, die mit dem Bezugszeichen 110 bezeichnet sind, werden sogenannte Freischalt-Code-Daten 111 generiert.

Die Freischalt-Code-Stelle 104 fordert von dem Trust-Center 101 ein sogenanntes Freischaltcodestelle-Signatur-Zertifikat 118 an. Unter Verwendung des öffentlichen Schlüssels 106 der Freischalt-Code-Stelle 104 und dem geheimen Schlüssel 103 des Trust-Centers 101 erzeugt das Trust-Center 101 das Freischaltcodestelle-Signatur-Zertifikat 118 auf der Basis des Public-Key-Verfahrens.

Ferner kann vorgesehen sein, dass die Software 113, die Signatur 114 und/oder eine hieraus abgeleitete Information oder Softwarenummer oder dgl. bei der Freischalt-Code-Stelle 104 hinterlegt ist und/oder ganz oder teilweise in das Freischaltcodestelle-Signatur-Zertifikat 118 eingeht. Das Freischaltcodestelle-Signatur-Zertifikat 118 weist insbesondere den öffentlichen Schlüssel 106 der Freischalt-Code-Stelle 104 und die vom Trust-Center 101 erzeugte Signatur 119 auf, anhand der überprüft werden kann, ob das Zertifikat 118 nach seiner „Unterzeichnung“ bzw. Signatur verändert oder manipuliert worden ist.

Bevorzugt weist das von dem Trust-Center 101 erzeugte Freischaltcodestelle-Signatur-Zertifikat 118 zudem ein oder mehrere Gültigkeitsbeschränkungen auf, die nicht explizit dargestellt sind.

Bei einer von dem Steuergerät 115 auf ihre Erfüllung hin überprüften Gültigkeitsbeschränkung im Freischaltcodestelle-Signatur-Zertifikat 118, kann es sich insbesondere um eine Beschränkung betreffend eine Betriebsstundenzahl, eine Lauf- bzw. Kilometer-Leistung, eine örtlich begrenzte Gültigkeit (in Bezug auf den Aufenthaltsort des Fahrzeugs), eine Zeitangabe oder Zeitdauer, ein oder mehrere Fahrzeugtypen, ein oder mehrere Steuergeräte oder Steuergerädetypen oder eine Fahrgestellnummer oder eine Steuergerätenummer handeln. Bevorzugt weist das Freischaltcodestelle-Signatur-Zertifikat eine Beschränkung der Verwendbarkeit auf eine bestimmte, das Steuergerät individualisierende Steuergerätenummer oder eine Fahrgestellnummer auf. Die Überprüfung der ein oder mehreren Gültigkeitsbeschränkungen bzw. Gültigkeitsvoraussetzungen erfolgt bevorzugt durch einen im Steuergerät 115 vorgesehenen, ablaufgesteuerten Mikroprozessor (nicht dargestellt), wobei dessen Ablaufsteuerung bzw. Software, entsprechend gestaltet ist.

Ein bevorzugter Freischalt-Code weist die folgenden ganz oder teilweise von dem Steuergerät 115 überprüfen und mit Referenzangaben verglichenen Informationsgruppen ganz oder teilweise auf: Software-Identifikation, Fahrgestellnummer und/oder Steuergerätenummer, Gültigkeitsbeschränkung, wie insbesondere eine absolute Zeitangabe, eine Betriebsstundenzahl, Identifikation des Nachfragers nach dem Freischaltcode, z.B. ein Fahrzeug-Händler oder ein Fahrzeugbesitzer, Identifikation der den Freischaltcode erzeugenden Freischaltcode-Stelle, Datum der Erzeugung und Signatur.

Beispielsweise kann die Beschränkung auch darin bestehen, dass die Freischalt-Code-Stelle Software und/oder Daten zur Verwendung durch ein im Fahrzeug vorgesehenes Navigationssystem, wie insbesondere Kartendaten oder dgl., nicht aber Software oder Daten zur Änderung der Motorsteuerung und/oder zur Ablaufsteuerung (besonders) sicherheitsrelevanter Steuergeräte freigeben kann.

Das von dem Trust-Center 101 erzeugte Freischaltcodestelle-Signatur-Zertifikat 118 und die Freischaltcode-Daten 111 sowie deren Signatur 112 werden in das Fahrzeug (nicht dargestellt) und nachfolgend in das betreffende Steuergerät 115 übertragen und dort gespeichert. Die Übertragung erfolgt bevorzugt drahtlos, wie insbesondere über ein Mobilfunknetz und/oder eine Internet-Verbindung.

Bevor das Steuergerät 115 die an das Steuergerät 115 übertragene Software 113 ausführt, prüft das Steuergerät 115 in einem dritten Schritt auf der Basis des Public-Key-Verfahrens unter Verwendung des Freischaltcodestelle-Signatur-Zertifikats 118, das den öffentlichen Schlüssel 106 der Freischaltcode-Stelle 104 und die Signatur 119 des Trust-Centers 101 aufweist, und unter Verwendung des im geschützten Speicher oder Speicherbereich 122 gespeicherten öffentlichen Schlüssels 102 des Trust-Centers 101, ob das Freischaltcodestelle-Signatur-Zertifikat 118 verändert bzw. manipuliert worden ist.

Falls dies nicht der Fall ist, prüft das Steuergerät 115 in einem vierten Schritt auf der Basis des Public-Key-Verfahrens unter Verwendung des öffentlichen Schlüssels 106 der Freischaltcodestelle-Stelle 104, der im dritten Schritt unter Verwendung des öffentlichen Schlüssels 102 des Trust-Centers 101 auf seine Unverändertheit hin überprüft worden ist, sowie unter Verwendung der Freischaltcode-Daten 111 und deren Signatur 112, ob die Freischaltcode-Daten 111 verändert bzw. manipuliert worden ist.

Bevorzugt wird beispielsweise von dem Steuergerät 115 bzw. einem in diesem vorgesehenen ablaufgesteuerten Mikroprozessor (nicht dargestellt) in einem fünften Schritt zudem überprüft, ob eine oder mehrere bevorzugt im Freischaltcodestelle-Signatur-Zertifikat 118 von dem Trust-Center 101 hinterlegte Gültigkeitsbeschränkungen bzw. Gültigkeitsvoraussetzungen erfüllt sind. Anderenfalls wird die Freigabe der Software oder deren Ablauf blockiert, wie insbesondere durch den Mikroprozessor.

Die positiv verlaufende Prüfung im dritten und vierten Schritt sowie ggf. die positive Prüfung im fünften Schritt, vorzugsweise von einem Prozessor (nicht dargestellt) des Steuergeräts, ist bei der beschriebenen, bevorzugten Ausführungsform der Erfindung

die hinreichende Voraussetzung, damit die Software 113 von dem Steuergerät 115 ausgeführt werden kann.

Verfahren zur Bereitstellung von Software zur Verwendung durch ein Steuergerät eines Fahrzeugs

Patentansprüche

1. Verfahren zur Bereitstellung von Software zur Verwendung durch ein Steuergerät eines Fahrzeugs, wie insbesondere ein Kraftfahrzeug oder Motorrad, **dadurch gekennzeichnet**, dass
 - die Software vor ihrer Verwendung durch das Steuergerät unter Verwendung des geheimen bzw. privaten Schlüssels einer Software-Signaturstelle im Rahmen eines Public-Key-Verfahrens gegen Verfälschung signiert wird, und
 - die signierte Software unter Verwendung des zu dem geheimen Schlüssel der Software-Signaturstelle komplementären öffentlichen Schlüssels auf ihre Unverfälschtheit hin überprüft wird.
2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, dass ein Software-Signatur-Zertifikat unter Verwendung des öffentlichen Schlüssels der Software-Signaturstelle und des geheimen Schlüssels einer Kontrollinstanz, eines sogenannten Trust-Centers, im Rahmen eines Public-Key-Verfahrens, erzeugt wird.
3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, dass ein Kontrollinstanz-Zertifikat bzw. Trust-Center-Zertifikat, im Rahmen eines Public-Key-Verfahrens, unter Verwendung des geheimen Schlüssels der Kontrollinstanz erzeugt wird.
4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet**, dass Freischaltcode-Daten unter Verwendung des geheimen Schlüssels einer Freischaltcode-Stelle, im Rahmen eines Public-Key-Verfahrens, signiert werden.
5. Verfahren nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet**, dass ein Freischaltcodestelle-Signatur-Zertifikat unter Verwendung des geheimen

Schlüssels der Kontrollinstanz, des Trust-Centers, im Rahmen eines Public-Key-Verfahrens, erzeugt wird.

6. Verfahren nach Anspruch 3, **dadurch gekennzeichnet**, dass das Trust-Center-Zertifikat in einer gegen Verfälschung und/oder Austausch geschützten Weise, wie in einem geschützten Speicher, Speicherbereich oder dgl., gespeichert wird, wie insbesondere in dem Steuergerät.
7. Verfahren nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet**, dass das Freischaltcodestelle-Signatur-Zertifikat, das Software-Signatur-Zertifikat, die Freischaltcode-Daten und deren Signatur sowie die Software und deren Signatur in dem Steuergerät gespeichert werden.
8. Verfahren nach einem der Ansprüche 2 oder 7, **dadurch gekennzeichnet**, dass das Software-Signatur-Zertifikat mit einer oder mehreren Gültigkeitsbeschränkungen, wie insbesondere eine Beschränkung auf einen oder mehrere Steuergerädetypen, versehen worden ist.
9. Verfahren nach einem der Ansprüche 5 oder 7, **dadurch gekennzeichnet**, dass das Freischaltcodestelle-Signatur-Zertifikat eine oder mehrere Gültigkeitsbeschränkungen aufweist, wie insbesondere eine Beschränkung auf ein bestimmtes Steuergerät, das beispielsweise anhand einer in diesem unveränderlich gespeicherten Nummer, Kennung oder dgl. individualisiert ist, oder eine Beschränkung auf die Fahrgestellnummer eines bestimmten Fahrzeugs.
10. Verfahren nach einem der Ansprüche 2 oder 8, **dadurch gekennzeichnet**, dass das Software-Signatur-Zertifikat im Rahmen eines Public-Key-Verfahrens unter Verwendung des öffentlichen Schlüssels des Trust-Centers auf Unverfälschtheit überprüft wird.
11. Verfahren nach einem der Ansprüche 1 bis 10, **dadurch gekennzeichnet**, dass die signierte Software im Rahmen eines Public-Key-Verfahrens unter

Verwendung des im Software-Signatur-Zertifikat enthaltenen öffentlichen Schlüssels der Softwaresignatur-Stelle auf Unverfälschtheit überprüft wird.

12. Verfahren nach einem der Ansprüche 5, 7 oder 9, **dadurch gekennzeichnet**, dass das Freischaltcodestelle-Signatur-Zertifikat im Rahmen eines Public-Key-Verfahrens unter Verwendung des öffentlichen Schlüssels des Trust-Centers auf Unverfälschtheit überprüft wird.
13. Verfahren nach Anspruch 4, **dadurch gekennzeichnet**, dass die signierten Freischaltcode-Daten im Rahmen eines Public-Key-Verfahrens unter Verwendung des im Freischaltcodestelle-Signatur-Zertifikats enthaltenen öffentlichen Schlüssels der Freischaltcodestelle auf Unverfälschtheit überprüft werden.
14. Verfahren nach einem der Ansprüche 1 bis 13, **dadurch gekennzeichnet**, dass das Steuergerät mit einem ablaufgesteuerten Mikroprozessor versehen ist, der eines der vorstehend beschriebenen Verfahren ausführt.
15. Steuergerät, insbesondere für ein Kraftfahrzeug oder Motorrad, **dadurch gekennzeichnet**, dass das Steuergerät ein Verfahren nach einem oder mehreren der vorstehenden Ansprüche ausführt.
16. Datenverarbeitungssystem, insbesondere für ein Kraftfahrzeug oder Motorrad, **dadurch gekennzeichnet**, dass das Datenverarbeitungssystem ein Verfahren nach einem oder mehreren der vorstehenden Ansprüche ausführt.
17. Computer-Programm-Produkt, insbesondere zur Ablaufsteuerung eines Steuergeräts oder eines Datenverarbeitungssystems eines Kraftfahrzeugs oder Motorrads, **dadurch gekennzeichnet**, dass das Computer-Programm-Produkt ein Verfahren nach einem oder mehreren der vorstehenden Ansprüche ausführt.
18. Datenträger, **dadurch gekennzeichnet**, dass er ein Computer-Programm-Produkt nach Anspruch 17 aufweist.

Verfahren zur Bereitstellung von Software zur Verwendung durch ein Steuergerät eines Fahrzeugs

Zusammenfassung

Die Erfindung betrifft insbesondere ein Verfahren zur Bereitstellung von Software zur Verwendung durch ein Steuergerät eines Fahrzeugs, wie insbesondere ein Kraftfahrzeug oder Motorrad.

Zur Verbesserung der Software/Hardware-Kombination, wie insbesondere eines Kraftfahrzeugs oder Personenkraftwagens, wird vorgeschlagen, dass die Software vor ihrer Verwendung durch das Steuergerät unter Verwendung des geheimen bzw. privaten Schlüssels einer Software-Signaturstelle im Rahmen eines Public-Key-Verfahrens gegen Verfälschung signiert wird, und die signierte Software unter Verwendung des zu dem geheimen Schlüssel der Software-Signaturstelle komplementären öffentlichen Schlüssels auf ihre Unverfälschtheit hin überprüft wird.

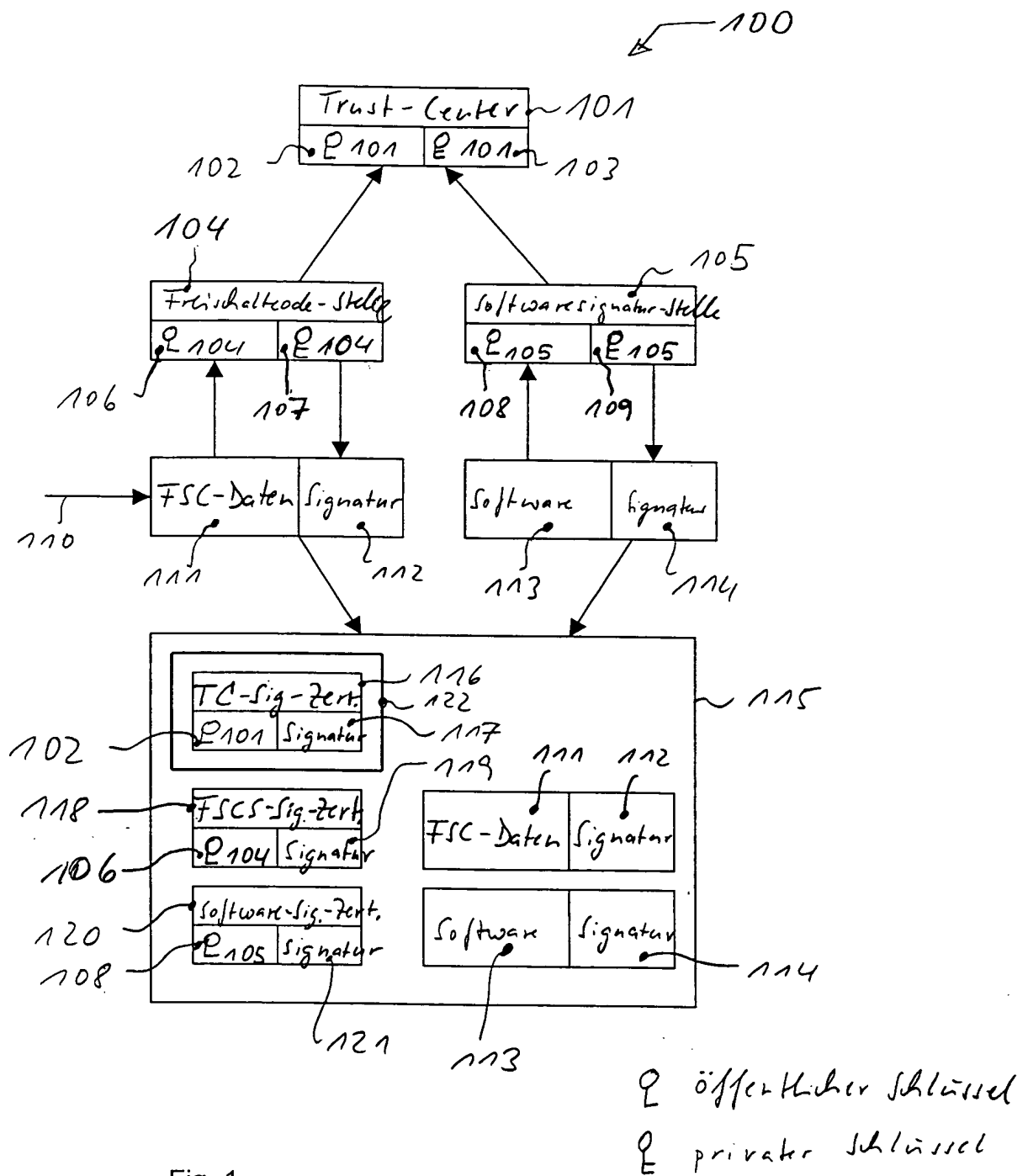


Fig. 1

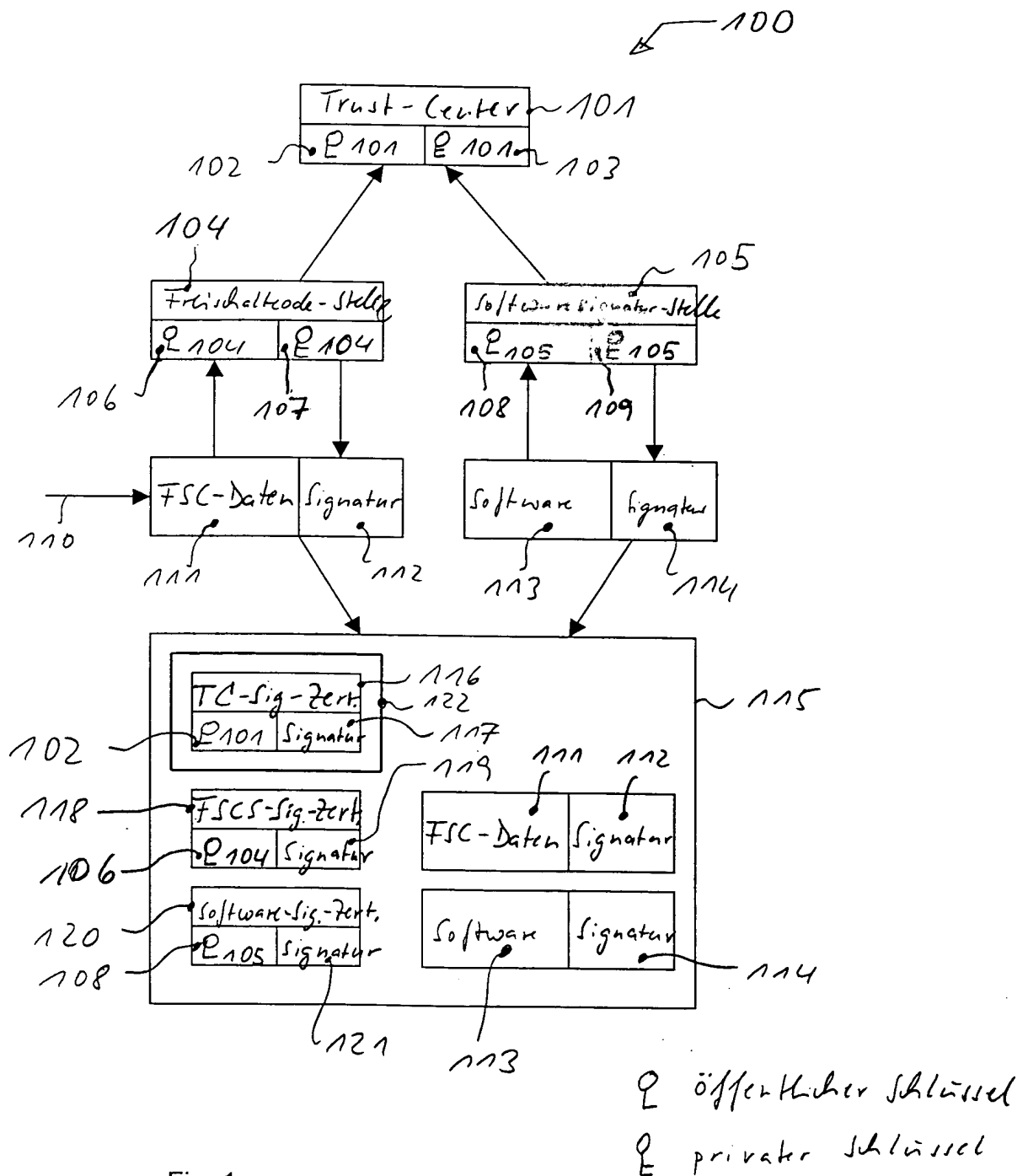


Fig. 1